This audit advisory report is distributed to recipients designated by the Inspector General and may be shared by those recipients with other FAO personnel for the purpose of taking action on the report. Neither the report nor any of its contents shall be disclosed to any third party unless such disclosure is expressly authorized by the Inspector General.

This audit advisory report is prepared solely for management and will not be subject to the report disclosure provisions contained in Section E of the Charter of the Office of the Inspector General.
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>2</td>
</tr>
<tr>
<td>OBJECTIVES</td>
<td>2</td>
</tr>
<tr>
<td>SCOPE AND METHODOLOGY</td>
<td>3</td>
</tr>
<tr>
<td>KEY OBSERVATIONS</td>
<td>4</td>
</tr>
<tr>
<td>ISSUES IDENTIFIED &amp; RECOMMENDATIONS</td>
<td>5-10</td>
</tr>
<tr>
<td>FRAUD SCENARIOS</td>
<td>11-27</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

In accordance with its 2022-2023 audit work plan, the Office of the Inspector General (OIG) conducted a fraud control assessment focusing on payments. The objectives of this audit advisory engagement were to raise management’s awareness of how the fraudster(s) could exploit the recurring control gaps in payment processes at decentralized offices to obtain financial gain or other benefits and recommend corrective actions at the corporate level. To develop more targeted controls, OIG came up with 16 fraud scenarios and highlighted possible preventive and detective controls at operational levels for each scenario.

KEY OBSERVATIONS

- In its audits of decentralized offices, OIG has observed that FAO operations have grown accustomed to some systemic and recurring internal control gaps in their internal control of payment processes. This has led to a reduced sense of alarm and has limited management’s ability to recognize red flags of fraud.
- Management tends to rationalize these control gaps with reasons such as lack of training, limited staffing capacity, the operational context, and system limitations. However, fraudsters could exploit such control gaps to mask their schemes.

CONCLUSION

While it is not feasible to prevent all acts of fraud, Management needs to be vigilant about such risks and be aware that the recurring control gaps in the payment processes are impeding them from preventing or detecting fraud cases when they occur. To alleviate the situation, OIG has made 13 advisory recommendations in this report for management’s consideration.

Mika Tapio
Inspector General
30 April 2024
The past audits of decentralized offices have revealed systemic and recurring internal control gaps in payment processes across the network, some of which increase the risk of fraud. While it is not feasible to fully prevent the risk of fraud, there are strategies for mitigating such risk depending on the level of complexity of the fraud schemes. To develop targeted controls countering fraud, it is crucial to be aware of how the fraudster(s) could exploit the control gaps to obtain financial gain or other benefits.

OBJECTIVES

The objectives of this audit advisory engagement were to:
- Raise management awareness of practices that allow fraudsters to mask their schemes;
- Highlight key internal control gaps and recommend actions at the corporate level to mitigate fraud risk in processing payments; and
- Identify possible fraud scenarios arising from the recurring control gaps in processing payments and accordingly propose possible preventive and detective controls at the operational level.

**INTRODUCTION**

**OBJECTIVES**

- Raise management awareness of the fraud schemes and risk exposure
- Highlight key internal control gaps
- Identify possible fraud scenarios in processing payments
- Propose mitigating actions at the corporate and operational level
SCOPE AND METHODOLOGY

The fraud control assessment considered the systemic and recurring internal control gaps identified in the audit reports of decentralized offices issued between 2018 and 2023. In addition, OIG took into account relevant investigation reports issued during the same period.

OIG developed possible fraud scenarios based on audit observations and typical workflows at decentralized offices. The fraud scenarios and the proposed controls were shared and/or discussed with relevant colleagues working at the Enterprise Risk Management team (ERM team), Finance Division (CSF), Project Support Services Division (PSS), the Office of the Emergencies and Resilience (OER), Shared Services Centre (CSLC) and the Travel Unit at headquarters.
KEY OBSERVATIONS

OIG observed that some bad practices have become widely acceptable, allowing fraudsters to mask their schemes. FAO management has grown accustomed to using workaround solutions to circumvent established rules and internal controls, leading to a diminished sense of alarm and limiting management’s ability to recognize red flags. Management often does not perceive exceptions as worrisome and tends to rationalize them by citing justifications such as lack of training, limited staffing capacity, the operational context, and system limitations. For instance:

- Vendor contact information and bank account numbers in GRMS are incomplete;
- Payee recorded in GRMS is not the actual payee;
- Multiple payments to different individuals are grouped and shown as one transaction in GRMS;
- Supporting documents of payments are not always accessible for remote review;
- Allowing manual bank transfers when Electronic Fund Transfer (EFT) functionality is available;
- Reconciliation of the bank accounts in General Ledger to the bank statements are done only once a year.

Furthermore, the reliance on budget holders to review and verify all transactions before approval is unrealistic mainly due to their competing priorities. Also, budget holders may not have a comprehensive knowledge of financial rules and procedures to detect anomalies.

OIG developed 16 fraud scenarios and identified some common control gaps among them that could be addressed through actions at the corporate level.
Rec 01: Campaigns on prohibited practices
CSF and CSLC to conduct campaigns on prohibited practices that are considered acceptable by country offices, including publishing them on the Intranet.

Rec 02: Training to identify red flags in processing payments
Training/Guidelines on verification of supporting documents for different types of payments.

ISSUES IDENTIFIED

Issue 01: Adoption of bad practices
1) Maintaining payees’ banking information outside GRMS;
2) Use of manual bank transfers when Electronic Fund Transfer (EFT) is available;
3) Allowing misrepresentation of payees’ information and payment amounts in GRMS
4) Payments to NSHR long after their contract’s expiry.

Issue 02: Inadequate verification of supporting documents for payments
Limited guidance available on the supporting evidence and checks required for different types of expenditures.
**ISSUES IDENTIFIED & RECOMMENDATIONS (CONT’D)**

**ISSUES IDENTIFIED**

**Issue 03: Supporting documents of payments are not available in GRMS**

The supporting documentation for payments is typically kept in hard copy and not uploaded in GRMS for review.

**Issue 04: Inadequate segregation of duties in processing payments**

The established workflows for issuance and settlement of advances allow an individual to single-handedly create and clear the advances in GRMS, relying on the review of Budget Holder as final control before payments. Some individuals are also granted conflicting GRMS responsibilities in processing payments.

**RECOMMENDATIONS**

**Rec 03: Need for a corporate solution for digitalization and filing of payment records**

CSF to establish a corporate solution for the digitalization and filing of supporting documents for payment records (either in GRMS or centralized storage) or escalate the risk exposure to senior management.

**Rec 04: Re-assessment of payment workflows and assignment of related GRMS responsibilities for segregation of duties**

CSF to re-assess workflows for payments including the issuance and settlement of advances for proper segregation of duties.

[OIG noted that there is an ongoing exercise by CSLC to address the issue of individuals having conflicting GRMS responsibilities]
**Issue 05: Over-reliance on budget holder and bank signatories to perform final checks before approving payments**

Budget holders and/or signatories often do not conduct a thorough review of payments’ supporting documentation before approving them, relying instead on other personnel’s review.

**Recommendation 05: Provide guidance and tools to Budget Holder**

CSF to provide the Budget Holders with tools and guidance on what needs to be reviewed and the data source to be used to detect discrepancies, anomalies and red flags before approving payments.

**Issue 06: Weaknesses in the bank reconciliation process**

No checks to detect discrepancies between the payee’s bank account number and name recorded in GRMS and in the bank statement. Reconciliation of the General Ledger’s bank accounts to the bank statement are done only once a year.

**Recommendation 06: Training to identify red flags in performing bank reconciliation**

CSF to provide training on reconciling the bank account in the General Ledger to the bank statement on a monthly basis and reviewing supporting documents to detect discrepancies between payees’ bank account numbers and names in GRMS and in the bank statement.

**Recommendation 07: Improve the monthly bank reconciliation procedures**

CSF to require Country Offices to reconcile the General Ledger bank account to the bank statement on a monthly basis.
Rec 08: Automated controls in GRMS

Recommended control features include:
1) GRMS notification to personnel whenever an advance is recorded or settled under their name;
2) Restrict the processing of payments using the payment method “Bank transfer” or “e-Banking” unless payees’ banking information is recorded in GRMS;
3) Enforce expense reports linking to a recorded advance.

Issue 07: Deficiencies in GRMS controls

1) No automated notification to personnel when an operational advance is recorded and settled under their name;
2) GRMS allows processing payments as “Bank transfer” or “e-Banking manual” without the banking information recorded in GRMS;
3) GRMS allows processing the payment of an expense report not linked to any advance.

Issue 08: No approvals needed for certain GRMS responsibilities

For example, the responsibility in GRMS to create Non-Staff Travelers (NST) is granted upon request and not subject to approval. Such records could be misused to process fraudulent payments in GRMS.

Rec 09: Assess GRMS responsibilities that could be granted without approvals

CSLC to review the list of GRMS responsibilities granted upon request and reassess the need for approvals. E.g. “FAO Travel Management NST Creation / Update.”
ISSUES IDENTIFIED

Issue 09: Lack of reconciliation between approved and actual cash transfers to beneficiaries

Incomplete/ineffective reconciliation process and documentary evidence to verify whether the beneficiaries paid by the financial service provider aligned with the approved list despite the requirements in MS 702.

Issue 10: Frequent non-compliance with segregation of duties requirements in managing Cash Transfers; and lack of a corporate system for beneficiary management

The requirements for segregation of duties are clearly stated in MS 702 but there are no effective controls to verify the compliance of Country Offices with such requirements. Also, in the absence of a corporate system for beneficiary management it is difficult to prevent and detect unauthorized changes to beneficiary records.

RECOMMENDATIONS

Rec 10: Implement monitoring controls over reconciliation of Cash Transfers

PSS to establish a corporate solution for the digitalization and filing of supporting documents for completed reconciliation of Cash Transfers to facilitate review or escalate the risk exposure to senior management.

Rec 11: Escalate the risk associated with the lack of segregation of duties and a corporate system for beneficiary management

Pending a corporate system on beneficiary management and effective controls over segregation of duties in handling Cash Transfers, senior management should be kept informed about the magnitude of the risk.
ISSUES IDENTIFIED & RECOMMENDATIONS (CONT’D)

ISSUES IDENTIFIED

Issue 11: Lack of clarity in second line functions
The roles and responsibilities of Second Line management function (e.g., CSF, CSLC, HQ Travel Unit, Regional Offices) in detecting red flags needs clarification. For example, the Headquarters Travel Unit stated it is not responsible to monitor travel related payments issued by decentralized offices, unless additional resources are provided.

Issue 12: Ineffective promulgation of internal control procedures
For example, CSF communicated some internal control procedures via emails which were not well documented for future references.

RECOMMENDATIONS

Rec 12: Clarification of the roles and responsibilities of the Second Line Management functions
CSF, CSLC, HQ Travel Unit, and Regional Offices are to clearly define and affirm their roles in implementing monitoring controls to spot red flags in payments. If an Office/Division is unable to fulfill this role due to a lack of resources, the Head should escalate the risk severity to the Core Leadership Team.

Rec 13: Communication of the issuance of internal control procedures
CSF to properly communicate the issuance of new or updated internal control procedures ensuring these are easily available to all relevant parties for future references.
# OVERVIEW OF THE FRAUD SCENARIOS

<table>
<thead>
<tr>
<th>FRAUD SCENARIO #</th>
<th>SHORT DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Misrepresentation of banking information</td>
</tr>
<tr>
<td>2</td>
<td>Misappropriation of funds through fraudulent Operational Advances</td>
</tr>
<tr>
<td>3</td>
<td>Misappropriation of funds through fraudulent expense reports by delinking an expense report to an outstanding advance</td>
</tr>
<tr>
<td>4</td>
<td>Misappropriation of funds through fraudulent expense reports by providing fake invoices of travel expenses</td>
</tr>
<tr>
<td>5</td>
<td>Falsification of invoices for reimbursement during settlement of operational advances</td>
</tr>
<tr>
<td>6</td>
<td>Misappropriation of funds through fraudulent payroll payments</td>
</tr>
<tr>
<td>7</td>
<td>Misappropriation of funds using falsified timesheets of former NSHR</td>
</tr>
<tr>
<td>8</td>
<td>Diversion of funds using falsified banking details</td>
</tr>
<tr>
<td>9</td>
<td>Fraudulent payments by recycling/editing supporting documents of other valid payments</td>
</tr>
<tr>
<td>10</td>
<td>Manipulation of accounting records to conceal embezzlement of funds by misusing &quot;Miscellaneous Receipts&quot;</td>
</tr>
<tr>
<td>11</td>
<td>Misappropriation of cash through omission in the recording of cash receipts</td>
</tr>
<tr>
<td>12</td>
<td>Misrepresentation of cash distribution to approved beneficiaries</td>
</tr>
<tr>
<td>13</td>
<td>Misappropriation of funds through the inclusion of fictitious project beneficiaries in payment instructions</td>
</tr>
<tr>
<td>14</td>
<td>Misappropriation of funds through fraudulent payments to Non-Staff Traveller</td>
</tr>
<tr>
<td>15</td>
<td>Misappropriation of funds through fraudulent request for Local Travel Authorization</td>
</tr>
<tr>
<td>16</td>
<td>Intentional overpayment of travel entitlements</td>
</tr>
</tbody>
</table>
### FRAUD SCENARIO #1

The Country Office keeps vendors’ banking information outside GRMS and uses it to process payments via bank transfers. The Country Office inadvertently directs a payment intended for a vendor to a fraudulent bank account after receiving a deceptive request from an external party to change the vendor’s banking information.

#### Fraud risk

Misrepresentation of banking information of a valid payee to divert funds.

#### Weaknesses identified in existing controls

GRMS allows processing of payments using the payment method “Bank transfer or e-Banking manual” although the vendors’ banking information was not recorded in the system. e.g. In 2023, there were 16,238 payments (USD 216 million) recorded in GRMS as “Bank transfers” and 23,729 payments (USD 52.8 million) recorded as “eBanking (Manual) although there were no records of vendors’ banking information in the system.

#### Possible preventive controls for consideration

- System controls requiring vendor’s banking information to be recorded in GRMS before processing payments through “Bank transfer or e-Banking manual.”
- CSF conducts campaigns and lists prohibited practices on the Intranet. For example, the maintenance of payee’s banking information outside GRMS.

#### Possible detective controls for consideration

N/A
FRAUD SCENARIO #2
Finance personnel (or someone with similar GRMS responsibilities) records fraudulent Operational Advance (OA) using other personnel's name in GRMS and settles it very quickly without being caught to avoid detection. Since the Country Office keeps external parties’ banking information (e.g., non-staff travelers) outside GRMS for payments via bank transfers, the fraudster makes the actual payment to an individual other than the recipient recorded in GRMS records.

Fraud risk
Misappropriation of funds through fraudulent OAs using the name of other personnel to record the OA in GRMS.

Weaknesses identified in existing controls
- GRMS does not notify the individual upon approval or settlement of an operational advance under his/her name in GRMS.
- Country Offices consider acceptable to misrepresent payment information in GRMS. E.g. recording advances in one employee’s name but paying another.
- Lack of segregation of duties between the individual creating, settling the advance and processing payments in GRMS and in the banking system.
- Budget holders and/or bank signatories rely on reviews conducted by other relevant personnel in approving payments. However, it is often unclear what was reviewed and the data source used to detect discrepancies, if any.
- GRMS allows processing payments via “Bank transfer or e-Banking manual” although the vendors’ banking information was not recorded in the system.
- Country Offices do not compare the payees’ names and bank accounts recorded in GRMS with information shown in the bank statement.
- Finance Personnel at the Country Office could approve an expense report in GRMS even without supporting documentation.

Possible preventive controls for consideration
- Automated GRMS notification to personnel whenever an operational advance is recorded under his/her name, and upon settlement.
- CSF conducts campaigns and lists prohibited practices on the Intranet. E.g. Misrepresenting payment information in GRMS.
- System controls requiring vendor’s banking information to be recorded in GRMS before processing payments through Bank transfer or e-Banking manual.

Possible detective controls for consideration
- AFAOR-Administration runs the IMIS report "Prepayments vs Expense Claims" and "FAO Outstanding Advances Report" monthly and sends details on the settled and outstanding advances to the related personnel for review.
- AFAOR-Administration analyses the settlement period of advances, with particular attention on advances that were settled within one to two days. The person responsible for conducting this analysis should be different than the one who is processing the advance in GRMS.
FRAUD SCENARIO #3

Finance personnel creates a fraudulent expense report to process payments by first applying/linking it to an outstanding advance [Vendor Advance (VA), Operational advance (OA) or Travel advance (TA)], but subsequently delinking it from the relevant advance to issue a fraudulent payment. Therefore, the advance will remain outstanding. In processing payments, the fraudster modifies the banking information to divert the payment to an individual other than the advance holder recorded in GRMS.

Fraud risk

Misappropriation of funds through fraudulent expense reports and unauthorized modification of banking information during payment.

Weaknesses identified in existing controls

- GRMS allows processing the payment of an expense report that is not linked to any advance.
- Lack of segregation of duties between the individuals applying the expense report to the advance and processing payments in GRMS and banking system.

In case the fraudster changes the payee's name,

- GRMS allows processing payments via “Bank transfer or e-Banking manual” although the vendors’ banking information was not recorded in the system.
- Country Offices do not compare the payees’ names and bank accounts recorded in GRMS with information shown in the bank statement.
- Finance personnel at the Country Office could approve an expense report in GRMS even without supporting documentation.

Possible preventive controls for consideration

- GRMS setup prohibits its user to unlink an expense report that has been applied to a prepayment.
- Only CSF or CSLC can unlink the applied expense report in GRMS. To unlink an applied expense report, Finance personnel at Country Offices should request CSF or CSLC for review and approval.
- CSF conducts campaigns and lists prohibited practices on the Intranet. For example, the maintenance of payee's banking information outside GRMS.

Possible detective controls for consideration

CSF conducts periodic analysis using the IMIS report “Prepayment vs Expense Claims” and looks out for expense reports with an invoice amount that significantly exceeds (e.g. over 50 percent or a minimum value of USD to be defined) of the approved advance amount. Further checks should be conducted to follow through the payments of such expense reports including verification of payee identity and banking information in the bank statement or bank remittance slips.
FRAUD SCENARIO #4
Traveler provides fake invoices for reimbursement of travel expenses during the settlement of TAs including claims under the category of “Other Expenses.”

Fraud risk
Misappropriation of funds through fraudulent expense reports and unauthorized modification of banking information during payment.

Weaknesses identified in existing controls
• Country Office personnel not adequately trained to perform expected controls on supporting documents justifying travel advances claims.
• Finance personnel at the Country Office could approve an expense report in GRMS even without supporting documentation.

Possible preventive controls for consideration
• Country Office personnel (Finance personnel/AFAOR-Administration/FAOR) should be trained on what needs to be reviewed to ensure the authenticity of the invoices before processing payments. Checks should be based on:
  o the address of the supplier (e.g. use of PO Box as address)
  o the lack of compliance with local statutory requirements (e.g. having a tax ID on invoices)
  o unusual invoice numbers (e.g. sequential invoices from the supplier submitted by the same personnel)
  o check suppliers’ website
In case of doubts, Country Office personnel should call or pay a visit to the vendor.
• AFAOR-Administration reviews and approves only on an exceptional basis “Other Expenses” claims, with proper supporting documents and clear justification.
• To establish a corporate solution for digitalization of payment records to allow for the remote review of payments supporting documentation.

Possible detective controls for consideration
The Regional Offices should designate responsibilities for performing monthly analysis to detect cases where the settled travel claims:
• significantly exceed (more than 50 percent) the approved advance amount to identify cases for further review and follow-up
• had claimed “Other expenses” on the travel advances
FRAUD SCENARIO #5
Operational advance holder provides fake invoices during the settlement of the advance.

Fraud risk
Falsification of invoices for reimbursement during settlement of operational advances.

Weaknesses identified in existing controls
- Country Office personnel not adequately trained to perform the expected reviews of the supporting documentation related to operational advances claims.
- Finance personnel at the Country Office could approve expense report in GRMS even without supporting documentation.

Possible preventive controls for consideration
- Country Office personnel (Finance personnel/AFAOR-Administration/FAOR) should be trained on what needs to be reviewed to ensure the authenticity of the invoices before processing payments. Checks should be based on:
  - the address of the supplier (e.g. use of PO Box as address)
  - the lack of compliance with local statutory requirements (e.g. having a tax ID on invoices)
  - unusual invoice numbers (e.g. sequential invoices from the supplier submitted by the same personnel)
  - check suppliers' website
In case of doubts, Country Office personnel should call or pay a visit to the vendor.
- To establish a corporate solution for digitalization of payment records to allow for the remote review of payments supporting documentation.

Possible detective controls for consideration
AFAOR-Administration runs the IMIS report "Prepayment vs Expense Claims" to identify individuals who had settled high amounts of operational advances, verifies completeness and validity of the supporting documents on a sample basis. This control should be conducted by a person other than the one processing the settlement of the advance.
## FRAUD SCENARIO #6

Finance personnel at the Country Office generates fictitious invoices to process the honorarium payment of NSHR who had already been paid through the payroll cycle, either to themselves or other individuals.

### Fraud risk

Misappropriation of funds through fraudulent payroll payments.

### Weaknesses identified in existing controls

Budget holders and/or bank signatories rely on reviews conducted by other relevant personnel in approving payments. However, it is often unclear what was reviewed and the data source used to detect discrepancies, if any.

### Possible preventive controls for consideration

Budget holders and/or bank signatories need training on fraud awareness and payment control procedures. The training should enable them to effectively review payment documentation, identify discrepancies, and recognize potential red flags. Emphasis should be placed on the minimum required documentation for review and specific elements to scrutinize.

### Possible detective controls for consideration

The Finance Unit at the Regional Office runs the IMIS “Payments from AP Report” on a monthly basis to identify all related payroll payments to personnel and compare it with their payroll records to detect duplicate payments, if any.
FRAUD SCENARIO #7
Finance personnel at the Country Office colludes with HR personnel to process payments by submitting timesheets on behalf of a former NSHR charging the unused days in the contract, and by changing the banking information of the former consultant to deviate funds either to themselves or other individuals.

Fraud risk
Misappropriation of funds using falsified timesheets of former NSHR.

Weaknesses identified in existing controls
• For terminated assignments, the system allows to process timecards and payments long after consultants have left the Organization.
• Not all employees have their banking information recorded in GRMS. Often, banking information is kept outside GRMS and entered manually by Finance personnel at the Country Office when processing payments. This facilitates making unauthorized changes to banking information.
• Budget holders and/or bank signatories rely on reviews conducted by other relevant personnel in approving payments. However, it is often unclear what was reviewed and the data source used to detect discrepancies, if any.

Possible preventive controls for consideration
• System controls enforcing the closure of NSHR contracts at the latest one month after the last day of the NSHR.
• System controls to disallow the submission of timecards one month after the contract NTE.
• Budget holders and/or bank signatories need training on fraud awareness and payment control procedures. The training should enable them to effectively review payment documentation, identify discrepancies, and recognize potential red flags. Emphasis should be placed on the minimum required documentation for review and specific elements to scrutinize.
• CSLC conducts campaigns and lists prohibited practices on the Intranet. E.g. processing of payments to NSHR long after their contract’s expiry.

Possible detective controls for consideration
Human Resource or Finance Personnel from Regional Office/HQ analyses payroll payments processed more than one month after the NTE of PSAs and consultants. This could be done by generating the “GRMS - NSHR Listing” report and pay particular attention to the difference between the dates shown in the column “Termination Date” and the “Final Processed Date”. If the difference exceeds one month, check if the NSHR have been rehired. Otherwise, assess the validity of the payment made after NTE using Payroll Reports.
FRAUD SCENARIO #8
Finance personnel at the Country Office makes unauthorized changes of the payment instruction in the e-Banking platform or the signed banking instruction letter to divert funds to an illegitimate recipient.

Fraud risk
Diversion of funds using falsified banking details.

Weaknesses identified in existing controls
- Lack of segregation of duties between the individual processing payments in GRMS and the one processing them in the banking system.
- Budget holders and/or bank signatories rely on reviews conducted by other relevant personnel in approving payments. However, it is often unclear what was reviewed and the data source used to detect discrepancies, if any.
- In countries without EFT, the bank signatories should review the payment instructions prior to disbursements. However, the fraudster could edit the scanned signed bank instruction letter.
- In countries with EFT, country offices do not maximize its use and instead continue processing payments through bank transfers or e-banking.
- Country Offices do not compare the payees’ names and bank accounts recorded in GRMS with information shown in the bank statement.

Possible preventive controls for consideration
- In countries with access to EFT, the AFAOR-Administration (with support of CSF and CSLC) ensures the use of EFT to process payments.
- At least two bank signatories are needed to authorise payment disbursements in the e-Banking platform. The bank signatories verify the details in payment instruction against the supporting documents before giving their approvals.
- If the e-Banking administrator right lies with the Country Office, the FAOR should assign these rights to personnel who has no role in the payment process and bank reconciliation. (e.g. IT personnel).
- CSF conducts campaigns and lists prohibited practices on the Intranet. E.g. not maximizing the use of EFT when available.

Possible detective controls for consideration
AFAOR-Administration reviews monthly bank reconciliations where the details of payment (e.g. the name of payee, payee banking information, amount of payment) as shown in bank statement are crosschecked with GRMS records. In cases where the bank statement does not show such information, the Country Office should request the bank remittance slips to facilitate the checks.
FRAUD SCENARIO #9

Finance personnel at the Country Office or project personnel recycle or alter legitimate supporting documents to process fraudulent payments.

Fraud risk
Fraudulent payments by recycling/editing supporting documents of other valid payments.

Weaknesses identified in existing controls

- Budget holders and/or bank signatories rely on reviews conducted by other relevant personnel in approving payments. However, it is often unclear what was reviewed and the data source used to detect discrepancies, if any.
- Lack of remote access to payments supporting documentation for possible detection of discrepancies.

Possible preventive controls for consideration

- The FAOR (Budget Holder) and AFAOR-Administration review the payment request by comparing the initial request with the one submitted for payment. This control might not be effective if the FAOR (Budget Holder) does not pay attention to the details and only relies on reviews by the Finance Unit and/or the Project manager.
- Budget holders and/or bank signatories need training on fraud awareness and payment control procedures. The training should enable them to effectively review payment documentation, identify discrepancies, and recognize potential red flags. Emphasis should be placed on the minimum required documentation for review and specific elements to scrutinize.
- To deter the risk of fraud pdf documents should be used, instead of Excel or Word.
- To establish a corporate solution for digitalization of payment records to allow for the remote review of payments supporting documentation.

Possible detective controls for consideration

Project managers analyse actual and expected expenditures by project. This control may not be effective if the fraudulent payments are spread in smaller amounts across different projects.
FRAUD SCENARIO #10

Finance personnel misuses the "Miscellaneous Receipt" function in GRMS to conceal fraudulent payments by creating fictitious receipt in GRMS to match the cash out in the Bank Statement.

Fraud risk

Manipulation of accounting records to conceal embezzlement of funds.

Weaknesses identified in existing controls

- Lack of segregation of duties between the individual creating the miscellaneous receipts in GRMS and the individual performing the bank reconciliation.
- The Country Office prepares monthly management letter focusing in ensuring all transactions shown in bank statement are reflected in GRMS without any checks to detect misuse of miscellaneous receipt function.
- There was no review by the second line management function to detect misuse of miscellaneous receipts.

Possible preventive controls for consideration

CSF to segregate the GRMS responsibilities between personnel performing bank reconciliation and those with the access right to issue/process "Miscellaneous Receipt."

Possible detective controls for consideration

Finance Personnel in Regional Office/HQ runs the “Cash Receipts” report in GRMS for all bank accounts and identifies offices with high volume/value (more than a specific number per year as defined by CSF) of miscellaneous receipts and those using miscellaneous receipt to record an expense.
**FRAUD SCENARIO # 11**

Misappropriation of cash through omission in the recording of cash receipts (cash receipt from for the rent of staff accommodation, cash receipt from sale of assets recorded as scrapped, reimbursement of private expense).

**Fraud risk**

Manipulation of accounting records to conceal embezzlement of funds.

**Weaknesses identified in existing controls**

Lack of segregation of duties between the individual receiving the cash payment, creating the miscellaneous receipts in GRMS and performing bank reconciliation.

**Possible preventive controls for consideration**

There are no effective controls to prevent the misappropriation of cash through omission in the recording of cash receipts.

**Possible detective controls for consideration**

- Finance personnel at Country Office reconciles the list of visitors/staff living in the compound with the rental income in GRMS.
- Finance personnel at Country Office verifies the evidence of scrapped assets; e.g. invoice or handover documents from the scrapping company.
FRAUD SCENARIO #12
Money vendor or mobile money network operator misappropriates funds by not disbursing cash as per FAO's instructions.

Fraud risk
Misrepresentation of cash distribution to approved beneficiaries.

Weaknesses identified in existing controls
- No/incomplete documentary evidence of cash received by project beneficiaries.
- Gaps in the use of biometrics data to verify project beneficiaries for cash transfers.
- Discrepancies in the reconciliation between approved and actual cash disbursements to beneficiaries.
- Corporate hotline for reporting misconduct including fraud is often not accessible or not well-communicated to the project beneficiaries.

Possible preventive controls for consideration
- FAOR requires the money vendor to use FAO tools to verify the identity of beneficiaries using prerecorded biometrics data. The digital tool should provide a report of the use of biometrics by the money vendor to distribute money to beneficiaries. This tool will control the existence of the beneficiaries but might not be effective to prevent underpayment of disbursed amount.
- The agreement signed with the money vendor service provider should request evidence of disbursements to the pre-approved beneficiaries.

Possible detective controls for consideration
- In the event that the Corporate Hotline is not accessible by beneficiaries, the FAOR establishes and maintains an effective and well-communicated local complaint mechanism for beneficiaries to report misconduct relating to cash transfers.
- Monitoring and Evaluation (M&E) personnel or a third-party monitoring verifies amount received by the approved beneficiaries e.g. call beneficiaries on sample basis to confirm the amount distributed.
- Project personnel reconciles the payment instructions with evidence of disbursements to the pre-approved beneficiaries. Reconciliation should be done line by line, instead of in total.
FRAUD SCENARIO #13

FAO personnel misappropriate funds by including fictitious project beneficiaries in the payment instructions to money vendor or mobile money network operators.

Fraud risk

Misappropriation of funds through the inclusion of fictitious project beneficiaries in payment instructions to financial service providers (money vendors or mobile money network operators).

Weaknesses identified in existing controls

• Non-compliance with the requirements for segregation of duties between beneficiary data management, programme/operations personnel and administration/finance personnel.
• The system access rights to modify approved beneficiaries' records has not been clearly defined to limit the access to such records.
• The Country Office does not reconcile the list of approved beneficiaries with the list of individuals that received cash transfers to detect discrepancies.

Possible preventive controls for consideration

• There are no effective preventive controls to ensure full compliance with the requirements for segregation of duties in handling cash transfers. However, the following could be done:
  o AFAOR-Programme defines system access right to modify payees' records to limited personnel.
  o System setup prevents unauthorized changes to payee records. The system should be able to provide audit trails of changes made, including the user, date, time and changes made.

Possible detective controls for consideration

• M&E personnel should receive the list of approved project beneficiaries directly from the approver. Subsequently, the M&E Personnel reconciles the list of approved beneficiaries with the list of individuals receiving cash.
• M&E personnel runs the report of changes in beneficiary data periodically and follows up on unauthorised or suspicious changes.
FRAUD SCENARIO #14 - Travel

Personnel with access (responsibilities) to create Non-Staff Travellers (NST) in GRMS includes a friendly party as NST to process fraudulent payments.

**Fraud risk**

Misappropriation of funds through fraudulent payments to NST.

**Weaknesses identified in existing controls**

- GRMS access rights (responsibilities) are granted to individuals without any approval. As of 5 February 2023, there are 1631 users holding the GRMS responsibility “FAO Travel Management NST Creation /Update”.
- Reviewers and/or signatories fail to conduct a comprehensive review of payment requests due to competing priorities. This lack of thorough scrutiny can contribute to oversight and potential approval of payments without a careful examination.

**Possible preventive controls for consideration**

- CSLC to define the approvals needed prior to granting GRMS responsibility to create NST.
- CSLC verifies if registration of NST in GRMS is duly supported by a valid ID, as required. Brief remarks about the reason for the creation of the NST should be documented.
- The reviewers (Finance personnel/AFAOR-Administration/FAOR) verify supporting documents for payment to NST before approval.
- CSF defines a threshold for each payment to NST. In case of payments for a higher amount, it would need pre-approval from CSF (similar to the threshold for Operational Advances).

**Possible detective controls for consideration**

- The Finance Unit at the Regional Office runs the IMIS - AP Payments Report, reviews and follows-up cases of: (1) NST names that do not resemble an individual; and (2) NST who received recurring and significant amounts of payments.
- The Shared Service Centre to review the IMIS – Vendor by OU report to assess if NST vendor’s information is legitimate by requesting supporting evidence of new NST records or recently changed on a sample basis.
FRAUD SCENARIO #15 - Travel

Project personnel submit a fraudulent request for Local Travel Authorization (LTA type: meeting local) or an operational advance to pay transport and meal allowances to participants of workshops organized by FAO. In such cases, the fraudster only needs to provide tampered attendance records of participants to justify the payments. This could be done by inflating the number of participants, or misrepresenting a workshop that did not take place.

**Fraud risk**

Misappropriation of funds through fraudulent request for Local Travel Authorization (type: Meeting Local).

**Weaknesses identified in existing controls**

- Incomplete data in the attendance sheets, and information included is difficult to be validated by an external reviewer.
- The Finance personnel at the Country Office could approve expense report in GRMS even without supporting documentation.

**Possible preventive controls for consideration**

- Project Team Leader reviews and approves the pre-established list of meeting participants. The list should clearly state participants’ names, the official titles (if applicable), the role of the individual attending the workshop (as a participant, trainer or technical advisory role), the contact information (mobile number) and the DSA amount to be paid.
- Project personnel obtains attendance sheet signed by the participants. The attendance sheet should show the printed names of approved participants and trainers but not the contact information or the amount payable. The participants should specify their contact and the amount received.
- To deter the risk of fraud, FAO personnel involved in the workshop should be informed that the Finance personnel at the Country Office will call the participants to verify the amount received.

**Possible detective controls for consideration**

Finance personnel verifies the attendance sheet against the pre-approved list. He/she calls the participants on sample basis, especially when there are discrepancies in the contact information or amounts paid as shown in the approved list and the attendance sheet. This may not be the most effective control, but it could have some deterring effects against fraudulent practices.
FRAUD SCENARIO #16 - Travel

Travel initiator colludes with the traveller to inflate DSA or other travel related entitlements either through unauthorized changes to DSA rates or inflating the number of days in exchange for money or other favours.

**Fraud risk**

Intentional overpayment of travel entitlements.

**Weaknesses identified in existing controls**

- Several DSA rates can be paid to individuals for the same itinerary. The GRMS responsibility “FAO Local Travel Country Admin” allows to apply different DSA rates for staff members, consultants, government staff, etc. who are traveling locally.
- There was no monitoring over the granting of the GRMS responsibility “FAO Local Travel Country Admin.” This responsibility can be assigned up to a maximum of two people per Operating Unit. As of March 2024, there were 16 Operating Units having more than two individuals with the “FAO Local Travel Country Admin” GRMS responsibility.
- There was no review of travel related reports by Second Line management function to detect misapplication of DSA rates.

**Possible preventive controls for consideration**

Direct supervisor of advance requester and Finance personnel at the Country Office review travel advance request and settlement prior to disbursement. For example, verifying the use of correct local DSA rates; e.g. reduced rates in PHP locations.

**Possible detective controls for consideration**

Travel Unit at HQ runs IMIS "Travel Details Report Summary" periodically and compares applied DSA rates with the correct DSA rates to detect overpayment.